IN THE UNITED STATES DISTRICT COURT FOR THE

NORTHERN DISTRICT OF OKLAHOMA

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | |
| | ) | |
| | ) | |
| Plaintiff, | ) | |
| | ) | |
| -vs- | ) | No. 15-CR-182-JHP |
| | ) | |
| | ) | |
| SCOTT FREDRICK ARTERBURY, | ) | |
| | ) | |
| Defendant. | ) | |

TRANSCRIPT OF MOTION HEARING

BEFORE THE HONORABLE PAUL J. CLEARY

UNITED STATES MAGISTRATE JUDGE

APRIL 25, 2016

A P P E A R A N C E S

Andrew J. Hofland, Assistant U.S. Attorney, 110 West Seventh Street, Suite 300, Tulsa, Oklahoma, 74119, attorney on behalf of the Plaintiff;

William P. Widell, Jr., Assistant Federal Public Defender, One West Third, Suite 1225, Tulsa, Oklahoma, 74103, attorney on behalf of the Defendant.

REPORTED BY: BRIAN P. NEIL, RMR-CRR
United States Court Reporter

Monday, April 25, 2016

* * * * *

DEPUTY COURT CLERK: This is Case No. 15-CR-182-JHP, USA v. Scott Fredrick Arterbury. Counsel, please state your appearances for the record.

MR. HOFLAND: Andrew J. Hofland for the United States, Your Honor.

THE COURT: Mr. Hofland.

MR. WIDELL: William Widell for Mr. Arterbury, Your Honor.

THE COURT: Okay. Let me ask a couple of things up front.

In the pleadings, there is a -- I think there's an ongoing reference to Web site A, and I guess there has been some effort not to identify the actual Web site but it's all over the place now. I think, as Mr. Widell pointed out, it's been the subject of a story in USA Today, it's been on all these Web sites and Motherboard and everything else.

Is there any reason why we wouldn't just refer to this as Playpen?

MR. HOFLAND: No, Your Honor, not at this point. And some of that was the time line we

were on when drafting began.

THE COURT: Sure.

MR. HOFLAND: But there's been a large gap of time now to where we're at so I would agree, Your Honor.

THE COURT: And so my intention is that when I get an order -- or an R & R out on this, I'll just refer to Playpen and the Tor network, I think is what we're talking about; right?

Okay. Who wants to start? Mr. Widell, it's your motion. Anything you want to add to what's already in your papers?

And let me say at the outset that the issue that I'm focused on, if you haven't gathered this from the minute order I entered last week, is the Rule 41 issue. The other two issues don't seem to me to rise to the level that I would -- I would suppress evidence based on the warrant on the basis of the description of the logo or the fact that the warrant related to all activating computers, but it's the Rule 41 issue that I'm most interested in.

MR. WIDELL: In the instant case, as opposed to Levin, the government concedes that the search took place in the Northern District of Oklahoma as opposed to the Eastern District of

Virginia. The government explains -- and this is on page 19 of its brief -- the government explains the nature of the instructions caused the search to be executed once packets of information arrived at the user's device, which is, of course, here in the Northern District. The information sought to be suppressed traveled from the user's device -- again, this is in the Northern District -- to the Playpen site, again on page 19 --

THE COURT: Is that where the -- when the NIT warrant is issued and they put this -- it's been referred to some opinions as "computer code," it's been described as "software" or "static extraction software" -- but when that information then is sent, the IP address, etcetera, does it go back to the Playpen site or does it go to another government computer, or do we know?

MR. WIDELL: I'm assuming the Playpen site because that's what it says in the government's brief.

THE COURT: And, Mr. Hofland --

MR. HOFLAND: It goes to another government computer in the Eastern District of Virginia. I think that's there in the briefings. I know it may not have been abundantly clear. But

it would require the computer -- the activating computer to send that information to another computer within the Eastern District.

THE COURT: Okay. That's kind of the impression I had, was that it was directed to send it to some other government computer. All right. But in any event, that's where it winds up is back in the Eastern District of Virginia.

MR. WIDELL: Rule 41(b)(2) allows a magistrate to issue a warrant for personal property outside the district if the personal property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed.

The Levin court looked at this exact issue and determined that the only object located within the Eastern District of Virginia was the government server, the activating computer was located outside the magistrate's jurisdiction, and the server in the Eastern District was not the device the government sought to search.

In its explanation of place to be searched, the NIT warrant made clear that the NIT would be used to obtain information from various activating computers; in other words, computers outside the

jurisdiction. The activating computer was the item to be searched.

Finally, we Levin court held that Rule 41 did not authorize the search because the actual property to be searched was not the NIT or the server on which it was located, but the user's computer outside the jurisdiction.

In the instant case, as in Levin, there's no indication that Mr. Arterbury's computer ever traveled to the Eastern District of Virginia. I know there's some discussion about if you link in, then perhaps you're in the Eastern District of Virginia.

But, again, the language of Rule 41(b)(2) says that the -- it's issue a warrant for personal property outside the district if the personal property is located within the district when the warrant itself was issued.

There's no indication that he was linked in or otherwise visibly present in the Eastern District at the time the warrant was issued. So I think the plain reading of the statute requires that Mr. Arterbury had to have been physically or -- I guess an argument could be made he would have to be linked in physically. Certainly there's no

type of international standard where he availed himself in the Eastern District at some point. In fact, when we look at Rule 41, we see Rule 41(b)(3) and (b)(5) actual authorize searches outside the jurisdiction. So I think that's further clarity that Rule 41(b)(2) and (4) are intended to do that.

THE COURT: Okay.

MR. WIDELL: Rule 41(b)(4). In its brief, the government also argues that (b)(4)'s tracking device provision authorizes a magistrate judge with authority to issue a warrant to install, again within the district, a tracking device.

So, again, the magistrate's authority is to issue a warrant to install some item that's already within the district. Again, the same argument: There's no indication that Mr. Arterbury's computer was either physically present at the time the warrant was issued or linked in.

The government again in its trial brief makes clear that NIT was not installed within the Eastern District of Virginia but rather within the Northern District of Oklahoma.

Additionally, Rule 41(b)(4) authorizes a tracking device for the sole purpose of tracking the movement of property. In fact, when we look at

41(b)(4) -- or rather Rule 41, tracking devices, it's defined in 18 U.S.C. 3117(b), and tracking device is defined just as it is in Rule 41, something that's intended to track movement. The warrant at issue -- the NIT doesn't track movement; it collects data. It, in no way, allows you to determine where Mr. Arterbury's computer was at a given point in time; it simply extracts computer data, sensitive data, from it.

And I think that's a point to raise in the Supreme Court's ruling in Riley v. California. So 41 authorizes tracking of objects. Riley v. California -- and that's 134 S.Ct. 2473, a 2014 case -- the Supreme Court held that devices that have significant data storage capacity are fundamentally different from other objects. With access to an object that has significant data storage capacity, like a cell phone, a smartphone, a tablet, a laptop, not only can you track where a device has been since the warrant was issued, but you can actually track where the device has been since the device was acquired.

Not only that, but it's different because the storage capacity -- well, Riley says quantitatively and qualitatively; quantitatively

because the immense storage capacity that these devices have; and qualitatively because we see not just an amount, but a type of data never considered before, maybe not just finite access, but a lifetime of access is out, data not just since he acquired the computer, but scanned on from the history of your life, financial records, medical records, Internet browser sites, revealing all sorts of personal information about an individual, political, financial, sexual.

So we're not talking about putting a tracking device on a car or bag and watching it travel from one street to the next; we're talking about putting malware onto a computer and extracting data.

Another thing I want to make clear, too, is that -- and I'll talk about this in a second -- but Levin didn't -- the Levin court didn't form its opinion on these ideas that I've just discussed. They say it's simply not a -- simply not a tracking device. Which, again, if you read the definition of a tracking device, it does not appear to be.

When we look at the committee notes from 2006 amendments, I think it says that the committee did not intend by this amendment to expand or

contract the definition of what might constitute a tracking device. So, again, that's 2006. My copy is page 193, Judge --

THE COURT: Okay.

MR. WIDELL: -- the first full paragraph on the left-hand column.

The Levin court cites the Tenth Circuit's recent case of United States v. Krueger as precedent for its determination that Rule 41(b)(4) did not authorize the warrant. The government argues in Krueger that the agent knew exactly where the computer was in another outlying jurisdiction, and that the fact that he understood initially exactly where the computer was and had the ability to go to that district and acquire a warrant somehow makes that case more egregious or this one less egregious.

In the instant case, the government argues that because agents, unlike in Krueger, lacked knowledge as to the location of the activating computer, they simply had no other choice other than to ask the magistrate to issue a warrant for computers that could be virtually anywhere in the world, and probably were, certainly outside the jurisdiction.

So, in other words, the government's argument is that Rule 41 should be read more liberally because there were limited options available to the agents. So there's nothing in Rule 41 to argue for such a liberal reading.

In fact, when we look at the antiterrorism section in (b)(3) and also (b)(5), we see that the committee already made those rules more liberal and allowed for that sort of thing. No cannon of statutory construction exists allowing a more liberal over a more literal reading.

In any event, the alternative to a more liberal reading, as pointed out in Levin, would have simply been to have the district court judge sign the second warrant. The Levin court points out that the district court judge was available to sign the initial warrant for the servers, I think, located in Florida. So they certainly had a course available to them that would have not necessitated us being here.

THE COURT: So the Rule 41 specifically talks about magistrate judges, and I know in -- I think even in Krueger, or maybe it's Levin, notes that it's not a limitation on the jurisdiction of a district judge. So had the district judge signed a

warrant like this, would it have been valid?

MR. WIDELL: I think so. Of course, Levin also says you can amend the rule, change the rule.

THE COURT: Which they're in the process of doing. And I think that's at the Justice Department's request, is it not?

MR. WIDELL: That would -- that would seem to be -- I don't know the answer to that question.

MR. HOFLAND: It is, Your Honor, in part.

THE COURT: And I believe it's up before the Supreme Court right now --

MR. HOFLAND: It is, Your Honor.

THE COURT: -- for review, yeah.

MR. WIDELL: So Levin didn't focus on a plain reading of the rule; Levin sort of simplified it and said it's not a tracking device. It didn't actually say it's not a tracking device because it doesn't meet the statutory definition, it extracts data rather than follows movement. What Levin said was the argument failed because the installation of the NIT, which we consider malware actually -- it seems to go on your computer and do something you

don't want it to -- occurred on the government-controlled computer in the Eastern District of Virginia.

Levin says the defendant was never in control of the government's computer, unlike the case in which a suspect drives car or carries a bag into the jurisdiction and then boards a train or plane to leave. If the installation occurred on the user's computer, the analogy likewise fails because the computer was never physically in the Eastern District of Virginia.

And, again, even if you want to read it a little more liberally to say that linking in at some point in the recent past created physical presence, again, the statute -- or the rule rather -- requires that Mr. Arterbury or the property, one or the other, be present, whichever they're seeking to track.

THE COURT: Is the property that we're focusing on here the computer or the information, or does it matter?

MR. WIDELL: I think it's the computer. I think that's -- you know, that's what the -- that's what the warrant says, the activating -- well, the warrant says the activating users, I

think, rather than the computer.

THE COURT: Right.

MR. WIDELL: So I think I had just assumed for whatever --

THE COURT: Because I think in one of the -- in the government's brief at one point they say that he brought the property or brought property to the Eastern District of Virginia, and I wanted to be clear. I mean, obviously, someone has reached into the Eastern District of Virginia. Whether they brought any property there, whether it be the computer -- obviously not the computer -- but whether they brought the IP address in some way into the Eastern District of Virginia, I don't know that there's any evidence of that.

MR. WIDELL: I think not. The actual Playpen site itself intentionally didn't acquire the IP address, so not until the NIT is loaded onto his computer does his computer send that information forward. And, again, in 2006, the committee notes indicate clearly that there's no intent to liberalize the definition of a rule.

Technical violation quickly. The Levin court made short work of that. The government in its briefing characterizes the violation as if, if

it exists at all, it's a technical one or a ministerial one. Clearly, it's a jurisdictional issue. I think the Levin court is correct, that a jurisdictional issue is not a technical issue, it's a substantive issue.

The Levin court found, you know, unlike some other cases, that even if it is or was considered -- characterized as a ministerial error, that prejudice did exist, just from the fact that if the magistrate hadn't -- you know, had followed the rule, the warrant wouldn't have been issued.

I think what Levin could have also pointed to was that prejudice means either the search might not have occurred -- not would not -- but might not have occurred or would not have been so abrasive. I think if the magistrate had followed the rule, not just the rule that says you can't go outside your jurisdiction, but the tracking device part, it would have been less abrasive in that only movement or possibly location would have been acquired and not all the other information was acquired as well.

So I think that we show prejudice by pointing out that the search might not have occurred and also the search would have certainly been less abrasive if the rule would have been

followed because the agents would have been allowed to collect sensitive data from the data storage device.

I think the object is the computer. The reason I think that is when you get a warrant for a car, now the information is not the car, the information is where the car went to; or the object is a bag, the information is not the bag but where the bag went.

Likewise, in this case, the object was Mr. Arterbury's computer. The information is supposed to be where his computer moved from the district to somewhere else.

THE COURT: If we -- if we assume here for a second that the warrant here doesn't comply with Rule 41 and that there is -- there is prejudice, then we're faced with the suppression issue.

The Michaud decision, which dealt with the same scenario we're dealing with here, the court simply said, well, the government would have gotten that IP address eventually anyway, it's like an unlisted phone number, and therefore, there's no prejudice, we don't need to suppress. Levin took a very different approach on that.

So what's the right answer?

MR. WIDELL: Two things. First, we don't have to show prejudice if we show substantive error, jurisdictional flaw; second, you know, I suppose it's possible the government might have gotten the IP address in another way, but we show prejudice again by the fact that the search should have been less abrasive than it was. If it's a -- if it's a substantive violation, then as the Levin court says, it's a void warrant. A void warrant is like no warrant at all.

THE COURT: And the good-faith exception doesn't apply?

MR. WIDELL: Good faith only applies to searches pursuant to warrant. So we don't even have to reach that if we determine that -- we don't even have to reach that if we determine that the error was jurisdictional, which, again, it seems to be. We reach good faith on the issue of the IP address possibly if we can't show prejudice.

So if we show error, we show no prejudice, now we're stuck with the IP address, then the argument, I suppose, is that there were -- there was other data collected, other than the IP address, that implicates Mr. Arterbury that should

certainly be suppressed.

Assuming by showing prejudice, either -- or assuming no need for prejudice because it's substantive or prejudice with a technical error, I think where we are with good faith is either if there's a -- if there's a -- if there's a valid warrant, I think we're in trouble, as far as good faith goes. If there's not a valid warrant; in other words, the warrant's void as opposed to voidable, then good faith simply doesn't apply and we don't need to pursue that issue.

THE COURT: Okay. Right.

MR. WIDELL: I think that's what I have to say in addition to the briefing on Rule 41. If you have anymore questions, I'll --

THE COURT: Okay. And is there anything -- I mean, the cases that I found out there that deal with our scenario, I got Michaud out of Washington and then Levin came down just last week, but I haven't seen any others out of the same sort of -- I'll call it the sting separation.

Is anybody aware of anything else? Mr. Hofland.

MR. HOFLAND: Yes, Your Honor. Pursuant to the court's minute order in this case to address

Levin, I also found three other opinions from three other districts that denied the motion to suppress. I've provided a courtesy copy to the court of those opinions and opposing counsel.

In chronological order, that's United States v. Michaud, M-i-c-h-a-u-d, from the Western District of Washington --

THE COURT: Right. That's the one we've talked about a little bit already.

MR. HOFLAND: Additionally, there in the Southern District of Ohio is United States v. Stamper, and that is a case out of the Southern District of Ohio, the Western Division, that is Case No. 15-CR-109 for that district.

And then additionally, there was a decision in the Seventh Circuit in the Eastern District of Wisconsin, which is United States v. Phillip Epich, E-p-i-c-h, for the Eastern District of Wisconsin, that's Case No. 15-CR-163.

I intend to address those. I know the court hasn't had much opportunity but --

THE COURT: Yeah. Why don't you step up and -- you folks have your pretrial tomorrow; correct?

MR. HOFLAND: Yes, Your Honor. It's our

understanding that the judge has already addressed the fact that we have an ability to respond to your report and recommendation. So my understanding is that it's going to be passed again.

THE COURT: All right. Good to know.

MR. HOFLAND: Your Honor, just taking up the issues --

THE COURT: Does everybody agree that 41(b)(3) and 41(b)(5) aren't applicable in any way here?

MR. HOFLAND: Yes.

THE COURT: We're only dealing with 41(b)(1), (2), or (4)?

MR. HOFLAND: Yes, Your Honor.

THE COURT: Okay.

MR. HOFLAND: So, first of all, when we're viewing Rule 41(b), I disagree with defense counsel's assertion that a strict application is the only application. The courts have found routinely that in cases of ambiguity, we're going to encourage or show a preference for warranted searches, as opposed to warrantless searches, in which we'll be creating incentive for law enforcement to cite exigency and attempt not to follow Rule 41 or seek warrants from magistrates.

And some citations that hold that very premise, originally -- well, the Supreme Court originally -- and this is an older case from 1977 -- in United States v. New York Telephone Company, that's 434 U.S. 159, that dealt with the Supreme Court upholding a 20-day search warrant for a pen register to collect dialed telephone number information despite the fact that the definition of "property" at the time did not include information and that the search be conducted within ten days.

So there, there was an issue where it outlasted the time in which it was supposed to be conducted and it didn't meet the technical definition because back then "property" wasn't defined as information.

THE COURT: Okay.

MR. HOFLAND: Regardless, the court explained in that case Rule 41 -- the Supreme Court -- Rule 41 is sufficiently flexible to include within its scope electronic intrusions authorized by a finding of probable cause and noticed that this flexible reading was bolstered by Rule 57(b) which provides, "If no procedure is specifically prescribed by the rule, the court may proceed in any lawful manner not inconsistent with

these rules or with any applicable statute."

So there is a history of reading Rule 41 more broadly assuming that it is, in the terms of the Supreme Court, not inconsistent with these rules or with any applicable statute.

There's also persuasive authority. The Ninth Circuit and the Seventh Circuit have taken it up more recently, the Ninth Circuit in the case United States v. Koyomejian, which is K-o-y-o-m-e-j-i-a-n, that's 970 F.2d 536 (9th Cir. 1992). The Ninth Circuit interpreted Rule 41 broadly to allow prospective warrants for video surveillance despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants.

And then the Seventh Circuit in 1984 in the case of United States v. Torres, T-o-r-r-e-s, 751 F.2d 875, (7th Cir. 1984), the Seventh Circuit observed that denying the court's authority to issue warrants for searches consistent with the Fourth Amendment would encourage warrantless searches justified by claims of exigency and -- quoting them -- they say, "Holding that federal courts have no power to issue warrants authorizing an investigative technique might simply validate

the conducting of surveillance without warrants. This would be a Pyrrhic victory for those who view the search warrant as a protection of the values in the Fourth Amendment."

And that last quote by the Seventh Circuit, I think, is especially important here. The bottom line is that technology is going to outpace the law. And so when law enforcement in a case like this does -- it's not out of a laziness -- which some people would comment on United States v. Krueger, that that was out of laziness knowing that there was property in the Western District of Oklahoma -- it's not out of laziness, it's out of the defendant, and defendants like him, and their choice of using encrypted end-to-end encryption to thwart law enforcement that we find ourselves with this issue.

To clarify a technical issue of what was already discussed, what we are talking about here under Rule 41 is information. That is the property that we're talking about. In Rule 41, as I included in my brief on page 19, the definition of "property" includes tangible objects or information, and that's what we're talking about searching here.

THE COURT: But isn't it -- but you're not going to get that information unless via the malware you seize control of Mr. Arterbury's computer and direct it to provide you that information.

MR. HOFLAND: Without -- without engaging in semantics, effectively, yes, Your Honor.

But what I would point out, which is, I think, a difference in your discussion with defense counsel just previously, is this information, an IP address, which is the crux of what was achieved here, the IP address is what allowed further investigative techniques to happen in this district and to obtain a particular search warrant for Mr. Arterbury's residence. So what we're really talking about is how do we achieve the IP address.

And as -- without calling an agent to further explain something that's outside the four corners of the affidavit, I can point the court's attention to Exhibit 1 of my brief, which is the NIT warrant itself. On pages 24 and 26, they specifically discuss that IP address information is information that a user, when he accesses a Web site readily gives up in order to receive contents

and packages of information back from the Web site.

So had we not been in an environment where there is end-to-end encryption used by the defendant, this is information that we could have used Rule 41(b)(1) to obtain a search warrant in the Eastern District of Virginia because on the server where the defendant is reaching to --

THE COURT: Right.

MR. HOFLAND: -- we see his IP address. That happens as a regular course of business technologically.

So when we're talking about this case with the end-to-end encryption but we start considering now Rule 41(b)(2) and (b)(4), we are -- we are looking for the exact information, which is covered by the definition under Rule 41(b), that the defendant willingly by his surfing conduct, or his Web surfing conduct, willingly gives to that server but for this encryption. So we really are talking about packets of information of the defendant reaching into the Eastern District of Virginia.

There's no doubt that we have zero evidence that Mr. Arterbury ever walked to the Eastern District of Virginia himself personally or that he schlepped his computer to the Eastern District of

Virginia. But what we're talking about is the bits of information that would have been available in the regular course of Web surfing but for the end-to-end encryption, really the information which is the IP address.

THE COURT: But if -- even if you captured even the encrypted IP address in the -- in the Eastern District of Virginia, you couldn't have done anything with it.

MR. HOFLAND: That's correct, Your Honor.

THE COURT: So whatever you've got is meaningless and useless unless you send the malware back to his computer in Oklahoma and say, okay, computer, we need for you to give us the IP address and this other information and send it back here.

MR. HOFLAND: That is correct, Your Honor. But in terms of --

THE COURT: I mean, it would be different -- I would agree with you if -- if what you had was some sort of -- you had captured in the Eastern District of Virginia an encrypted IP address, which you then proceeded to de-encrypt and had the property but it had been hidden, but through use of a warrant or some technique you were

able to get the information that had been brought in. But that's not case.

MR. HOFLAND: You're correct, Your Honor. And as I think is laid out sufficiently in Exhibit 1, the NIT warrant itself, simply not possible.

THE COURT: Right.

MR. HOFLAND: No matter what he did, based upon the way this end-to-end encryption worked with these nodes, it's simply not possible for us to de-encrypt the information. Even the last exit node or the server itself has no idea who the activating user is on the other side of these relay nodes.

THE COURT: And that's the problem I have with Michaud, is when the judge without any citation says, well, this is just like an unlisted phone number and they would have gotten at it eventually anyway, I've got a problem with that, particularly because the McFarland affidavit is completely contradictory to that.

MR. HOFLAND: Well, yes, Your Honor. I think that gets to prejudice, which I'd like to address in a moment.

THE COURT: Okay. Sure.

MR. HOFLAND: But just for framework-wise --

THE COURT: Sure.

MR. HOFLAND: -- I want to talk about Rule 41(b)(2) and (b)(4).

THE COURT: Okay.

MR. HOFLAND: I know the Levin court gives it somewhat sort shrift. There are very short paragraphs where he simply denies out of hand that these are applicable. But when we're talking about packets of information that are coming into the Eastern District of Virginia, I think that is helpful for us to view the framework that's currently in place. And granted it was written at a time where we didn't have this particular issue of end-to-end encryption, but when we understand, looking back at those other cases I cited, as to even though technology may be ahead of the rule, are we within the spirit or the scope of the rule?

I think that this is not even a violation of Rule 41(b)(2) and (b)(4), (b)(2) being that if the property, meaning the tangible object or the information that is to be sought, is within the Eastern District of Virginia, which I submit that it was because of his surfing habits, that he was

giving something through his computer to that server to be able to retrieve something back, which is this IP address, that because that puts Mr. Arterbury in -- or that information in the Eastern District of Virginia; and then under (b)(2) we're allowed to, if that information is going to move out of the Eastern District of Virginia, to track it or to search where that information may go, which is what (b)(2) posits, and that's exactly what happens in this case.

Now, again, it's not going to be a perfect fit because we're talking about something that was you know invented after these rules were created.

THE COURT: Right.

MR. HOFLAND: But cognitively when we look at what we talked about before, it's effectively the same thing that we're having to search here but we're authorizing a search where this information or property goes, which in this case is back to the Northern District of Oklahoma.

And simply another way, in almost the penumbra of (b)(1), (b)(2), and (b)(4) when read together, we also have the tracking device analogy, which I think is actually very apropos. I gave my analogy to it with the Holland Tunnel.

THE COURT: The Holland Tunnel.

MR. HOFLAND: But, I mean, I think that's right. We can put a tracker on something in one district, we can have technical reasons why it doesn't continue to be -- or give us a homing signal, but when it travels in another district we can continue to retrieve that location information.

As put in my brief on page 19, the tracking device is considered either a mechanical or electronic device. That's effectively what this is, granted all in a digital or cyberworld. Attached to the packets of information Mr. Arterbury was receiving was these instructions or this code, and so that is our tracking device, the electronic device, that's attached to digital information that traveled back to the Northern District of Oklahoma where the path was absconded from us because it's an end-to-end encryption, but we see it going out and we see it where it ends up, just as if it pulled out on the other side of the Holland Tunnel.

THE COURT: If it was just tracking, you would track the information back to the Northern District of Oklahoma and the tracking portion would be over, but then the next step is the malware

seizes control of the computer and sends information back to the Eastern District of Virginia that Mr. Arterbury never intended to happen.

MR. HOFLAND: Well, the key, Your Honor, is, what information are we looking for? Because this is where we differ from what the defense's brief talks about in In Re: Warrant from the Southern District of Texas.

THE COURT: Right, right. Where they wouldn't issue the warrant.

MR. HOFLAND: That was an out-and-out -- the proposed warrant was an out-and-out search of the computer, much like we would forensically do to say file structure and images and things on the computer.

Here, this is very different because the scope of what was being asked for is what the computer emits once he travels on the Internet to a Web site, which is the IP address. This is information that the defendant freely gives up by surfing the Internet anytime he connects to the Internet.

So really when we're talking about searching the computer, it's not for searching

underlying file structure, anything that he would have a reasonable expectation of privacy in; it's simply another means of showing that information that he's pulling out every time he travels out just in an unencrypted manner.

So it's not a perfect fit to say this is --

THE COURT: If it was a perfect fit, you wouldn't -- the government wouldn't be trying to amend Rule 41 right now to solve the problem.

MR. HOFLAND: That is true, Your Honor. At some point we need to catch up in the same way that after the Supreme Court decision we said that property included information. At some point we need to catch up.

And so -- but I don't think it's because of the fact that they're creating an on-point -- or trying to create an on-point Rule 41, I guess, (b)(6) or something to address this situation, it doesn't mean that it's not currently addressed.

The reason why I think that's the most fair reading of this, in addition to the case law where we talk about the liberal construction, is because when we have law-enforcement agents who are trying to identify illegal criminal activity -- and we talked a little bit about the horrors of what's

going on as far as new content and the creation of child pornography being really the gravity or the gravamen of what this site was for, people to create and share -- we want law enforcement to be able to try to use the courts to achieve information in these sorts of cases.

And so what do we have? We have a law-enforcement agent in the Eastern District Virginia at that point coming to the only place where it would make any sense for anybody to go, as far as a jurisdiction, which is the Eastern District of Virginia where the server was located, and attempting to retrieve court authorization to do the very thing that they did which the court then approved.

So to then now deny that -- or grant a motion to suppress is to say it should -- we shouldn't try to use Rule 41 or that somehow Rule 41 simply didn't allow us to investigate these cases. And that simply can't be the sensical reading in light of the totality of the case law and in light of the way that Rule 41 is structured was that simply some people are going to be outside of the -- outside of our law when we seek court authorization.

THE COURT: What happens, though, when a magistrate judge is presented a warrant like this and has no idea really where the packet of information or the computer ultimately lies?

I mean, when this magistrate judge signed the NIT warrant, she didn't know whether the ultimate target was going to be in the Eastern District of Virginia, in which case we're probably not having this discussion, or it's outside the Eastern District of Virginia but inside the United States, or it's outside the United States.

What does -- what difference does it make in your analysis? Under Rule 41, does it make any difference at all?

MR. HOFLAND: Your Honor, Rule 41(b) provides for extraterritorial jurisdiction on search warrants, and that's what (b)(2) and (b)(4) and then under very particularly circumstances, (b)(3) and (b)(5) contemplate.

So when we're talking about whether or not Rule 41(b) is meant to allow extraterritorial jurisdiction over warrants, the answer is yes. And in reading it in a fair light, in a light that we're reviewing new technology in terms of the framework we have, I think it does authorize it

even thought she didn't know where it went.

You know, another reason why we can say why we know that the federal courts allow this -- or contemplate this sort of investigative technique is we also have anticipatory warrants; right? So if we were to want to search a -- we have a drug mule who's a cooperator, and we know that the drug mule is going to be going on a run but he's not told where he's going, we can also seek anticipatory warrants that would allow when a triggering event occurs, like when the drug warrant is -- or excuse me -- when the drug mule is finally given the address or directions on the freeway as to where he's supposed to go, we can also have warrants that allow us to search that location given anticipatorily, even though we don't know at the time where the person is necessarily going.

So, again, when we look at all the different ways that there is codified or, in the rules at least, an ability to look for information from outside the district that you're applying for it in, we see that the court does authorize these. They're not -- they're not as commonplace but they do authorize these types of warrants.

THE COURT: But the fact that 41(b)(3)

very specifically says when -- I mean, when you look at 41(b) overall, there's a territorial limit placed on the power of a magistrate judge to issue a warrant.

Now, you get to 41(b)(3) and the rule says, now, wait a minute, if it's terrorism, domestic or international, all bets are off and you can issue a warrant to go anywhere; right?

MR. HOFLAND: Yes, Your Honor.

THE COURT: Does the fact -- I mean, why wouldn't they have included child pornography cases in 41(b)(3), if that's what they intended? I mean, if we're going to do away with any sort of territorial limit in situations like this, I mean, it seems like they saw the need to do it and they put it in (b)(3).

MR. HOFLAND: Your Honor, so Rule 41(b) is going to have amendments based upon an ill that's trying to be cured, I guess, such as the telephone company then defining property differently.

Clearly what we're talking about in that situation, when we're talking about counterterrorism, is exigency but now codified; right? So we already can seek -- not need a

warrant under exigent circumstances but, again, there's a preference to get a warrant.

So what they did is effectively when we're talking about counterterrorism, they said, this is an exigent circumstance, but no longer do we want you to worry about whether or not you should not seek a warrant. We prefer you do seek a warrant and now we're going to give you officially an avenue to do so you stop doing exigent circumstances, and that way we can -- the courts can have authorization which will likely make it more bulletproof.

The fact that now there's a differing type of technology, which is making what normally would be a Rule 41(b)(1) warrant pretty simple, let's just search the server and find his IP address, because now there's a proposed change on that doesn't mean it's simply not there because (b)(3)'s there and it doesn't contemplate child pornography.

And to that point about both Rule 41 and the preference to Rule 41, but then also kind of alternatively the prejudice, in this case when we're talking about whether or not this should be suppressed, I think this court can hang its hat on exigent circumstances.

There's a footnote at the end of my brief, and due to, I guess, page limitations I don't know if the issue was fully fleshed out, but in that footnote at the end of my brief we talk about exigent circumstances. Within Exhibit 1 of our brief, where it is the NIT search warrant itself, it talks about the great harm that's happened and effectively that the information is fleeting. People are harming children in realtime. People's information are traveling in through this relay node and leaving. And if we don't capture it in that two-week period of time, those people effectively got away with it.

THE COURT: Well, but it bothers me a little bit, the exigent circumstances argument, when it's the government that left the server and let this continue on. I mean, I know how strictly you guys are with defense counsel when they want to come in in child pornography cases and look at what the evidence is and they're not allowed to take it out and they have to sketch it and all that.

And here we are with the government saying, well, we're going to let this -- we're going to let this operation continue and let people traffic in child pornography for awhile in the hopes that we

can catch many, if not all, of them.

MR. HOFLAND: Yes, Your Honor. And certainly for the decision-makers that took out this warrant it was a difficult decision. What I think is addressed within the warrant itself is the concept that when you take one of these sites down, another one pops of immediately in its place.

THE COURT: Yeah.

MR. HOFLAND: And so dealt with the -- given the option in this particular circumstance of taking down this one Web site administer and then taking down the site and then letting folks share on the next marketplace that was going to pop up like -- and have a game of whack-a-mole, they decided that they were going to attempt to find the individual users that are sharing in child pornography, even individual users that are harming children.

I can tell you that even out of Operation Pacifier, based upon the search warrants, they were able to rescue kids who were being abused in realtime. And if the court's interested, I can bring out a supplemental exhibit which provides a summary of some of those realtime curers that have already been -- the rule time ails which have

already been cured by the Operation Pacifier, which really does raise the question about exigent circumstances in the content and what's going on in that particular case.

So I think I've explained why I think Rule 41, based upon the way that it should be read, is as flexible and in a more liberal construction than a strict construction based on the history of it, and then looking at Rule 41(b)(1), (b)(2), and (b)(4), why under these circumstances we should not find a violation of Rule 41.

THE COURT: Now, the NIT warrant when it was presented to the magistrate judge very clearly said it was to search and seize property located within the Eastern District of Virginia.

MR. HOFLAND: And that -- I believe it also discusses, you know, the activating users.

THE COURT: Right.

MR. HOFLAND: So I think maybe it might have stated Rule 41(b)(1), which in terms of the IP address is true, that is information that traveled into the Eastern District of Virginia. But because they're talking about the authorizing computer as well --

THE COURT: Did this IP address even

encrypted travel into the Eastern District of Virginia? Because I thought from McFarland's affidavit he was saying that all they could do with the information that was in the Eastern District of Virginia is track it back to the last exit node, and they didn't have the ability to go any farther without the NIT process.

MR. HOFLAND: That's correct, Your Honor.

So what we're talking about, I guess, is, is information or are packets of data traveling from the defendant's computer into the Eastern District of Virginia? And the answer is yes. There's no way for him to view anything on that server if he's not reaching out through the Internet, if he's not sending packets of data.

Simply put, there's no way for me to download from any server on the Internet without sending something out, sending packets of information out.

THE COURT: Right.

MR. HOFLAND: So what happened here is, the routine information that's sent out -- and, again --

THE COURT: The routine packet would

include the IP address?

MR. HOFLAND: It does. I mean, as he's searching, even on the Tor network, what's going out are certain statistics about his computer, the IP address, the MAC address, other items that say what's coming out across the Internet. And just what happens is, from the entry node to the exit node and on the relays, they encrypt another level and another level and another level so that what comes out of the exit node is still that information, it's just highly encrypted.

So the defendant did reach into the Eastern District of Virginia. It's just when he reached into the Eastern District of Virginia, it was still an IP address but an IP address that was heavily encrypted and unable to be de-encrypted without some further instructions or code.

So --

THE COURT: But then, you couldn't take what was in the Eastern District of Virginia, even with some sort of NIT technique, and de-encrypt it in the Eastern District of Virginia?

MR. HOFLAND: Not --

THE COURT: You had to send something back to the Northern District of Oklahoma saying to

the computer, okay, we can't figure this out, computer, gather up this information and send it to this computer in the Eastern District of Virginia?

MR. HOFLAND: Yes, Your Honor.

So even if we -- even if we say that to the letter of Rule 41(b), there is nothing that specifically addresses what happened in this case, it really is a technical violation, not a substantive one.

And I understand what the judge said in the Levin court, but he is an outlier with the other courts that have denied the motion to suppress. What's interesting as well about Levin's decision is Levin does cite to Krueger --

THE COURT: A lot.

MR. HOFLAND: -- which is a Tenth Circuit court --

THE COURT: Right.

MR. HOFLAND: -- and he cites to -- and I'm going to butcher his name -- Gorsuch's --

THE COURT: Gorsuch. Judge Gorsuch, yeah.

MR. HOFLAND: -- Judge Gorsuch's concurrence, but the analysis that occurs in Krueger is the analysis given to us in the Tenth

Circuit, the standing analysis, in Pennington.

THE COURT: Right.

MR. HOFLAND: So in the Tenth Circuit, what we have here is in the instance of a Rule 41 violation, we go through a certain analysis.

Levin -- the Levin court doesn't touch on that analysis; it simply says this was not technical, simply there's no jurisdiction, we have no warrant. But the problem is that even the case that he cited not from his district but, our district here -- or our circuit --

THE COURT: Right.

MR. HOFLAND: -- is an analysis where in Krueger they went through the steps. And even though Krueger had a similar type problem with the specifics of Rule 41(b)(1), (2) -- well, (b)(1), which is a question of jurisdiction, the Tenth Circuit still went through all of those Rule 41 violation tests, which tell me that at least in the Tenth Circuit this is -- we have a framework for analyzing Rule 41 violations and it does not distinguish when we analyze Rule 41 violations from Rule 41(a), from Rule 41(b). These are all parts of Rule 41 violations, and there is no distinction within the Tenth Circuit between the fact that

(b)(1) through (5) have these jurisdictional requirements versus (a) has other technical requirements about it. They're all technical violations of Rule 41.

THE COURT: I don't know that I agree with that. Because in Krueger in footnote 7, the court discusses the fact that we've addressed over the years many provisions of Rule 41, never concluding that the alleged 41 violation justified suppression; however, those were 41(c), 41(d), (e). At the last, it says, "Because none of these cases addressed Rule 41(b)(1), which is unique from other provisions of Rule 41 because it implicates substantive judicial authority, they offer limited guidance here."

So it sounds to me like they are drawing a very substantive distinction between 41(b) and the fact that it goes right to the heart of the authority to issue the warrant versus some of the other provisions, where if a copy isn't signed properly or something isn't filed directly on time or something like that, that wouldn't affect -- those sorts of violations would not have affected whether the search was -- would have ever happened.

MR. HOFLAND: I understand, Your Honor.

And you did refresh my recollection about Krueger, that they do -- they do contemplate the idea of the same situation that we're in, that something like this we don't know we've taken up before.

THE COURT: Yeah.

MR. HOFLAND: But even though they drop that footnote, Krueger still conducts a full Pennington analysis, Pennington being the prior case that gives us violations of Rule 41.

THE COURT: Okay.

MR. HOFLAND: So if the Tenth Circuit truly believed that Rule 41(b) raised a substantive-level violation, then we would have seen an opinion that looked closer to Levin and did continue to conduct the analysis of, was there a violation, was it constitutional in nature; and if not, do we have prejudice or do we have intentional and deliberate disregard?

What's interesting, I think, for this court in looking at the other district courts, at least persuasively that are taking up this issue, is in the Western District of Washington their circuit has a Rule 41 analytical framework that is almost identical to ours.

THE COURT: Right.

MR. HOFLAND: In theirs, they conduct the Rule 41 violation analysis to say, was Rule 41 violated? And in Michaud, they say it was a technical violation but it was within the spirit of the law. They say it was certainly not a constitutional magnitude because all of the requirements of the Fourth Amendment were complied with which, from our prior discussion, that looks like that's not at issue here really or it doesn't trouble this court. And so it takes up the question of prejudice or intentional and deliberate disregard and it says that neither were met, there is no prejudice, which I'll address in a second.

But what's also -- United States v. Stamper, the other case from the Southern District of Ohio, they, too, have a framework -- and now we're talking about the Sixth and the -- Sixth and the Ninth Circuit --

THE COURT: Ninth in the Michaud case.

MR. HOFLAND: Yes, Your Honor.

So in the Southern District of Ohio, their circuit case law also mirrors what we have in Pennington, which is a Rule 41 violation to be -- determine the questions of, is there a technical -- is there a violation, is it constitutional in

nature, and then is there prejudice or intentional or deliberate disregard?

So on two of those cases that have taken up this very issue, they walk through the steps of Rule 41, because even though we're talking about a Rule 41(b) violation, they don't see it the way that the judge in Levin does, which is we go no further, we have no jurisdiction, all stop.

The Seventh Circuit in United States v. Epich, they don't particularly address that Rule 41 framework. I think theirs is a little bit different. They simply say it's not constitutional in magnitude and the good-faith exception prevails here.

So all of these other courts, with the exception of Levin being the outlier, they allow us to look at good faith and they allow us to look at prejudice or intentional and deliberate disregard, and only Levin -- and I haven't been able to do a full survey of their circuit law -- but only Levin is the one who simply says, all stop, we don't even reach the issue.

THE COURT: Yeah. I mean, Levin seems to say that there are cases out there in support for the idea that if the -- if the warrant is void

ab initio, good faith is not going to be -- not going to be applicable.

MR. HOFLAND: Right. That's not present in this -- in the other decisions that deny the motion to suppress.

THE COURT: No, I wouldn't think so.

MR. HOFLAND: Right. And Levin -- and Levin simply is not in our circuit and doesn't have the Rule 41 framework that we have.

THE COURT: Right.

MR. HOFLAND: So understanding that the first part of Levin is -- we'll assume here that there is a Rule 41 technical violation, but it's not constitutional in nature, so then the question comes down to prejudice or intentional and deliberate disregard.

I think we can pretty quickly put aside intentional or reckless or deliberate disregard for the rules because very clearly from the warrant, and otherwise, we see that law enforcement is doing the best they can without knowing where the activating user is based upon the conduct of the activating user.

THE COURT: What if the government agent had -- and obviously I don't know how long the

proposed amendment to Rule 41 has been in the works -- but what if the government agent in Virginia had gone to the court and said, we have to have a district judge issue this warrant --

MR. HOFLAND: Well --

THE COURT: -- the magistrate judge isn't going to have authority, or we are concerned about the magistrate judge's authority to issue the warrant under Rule 41(b); therefore, we're asking a district judge to do it because -- and Mr. Widell seemed to agree with the idea that in that case there wouldn't be the same limitation.

MR. HOFLAND: Your Honor, the United States respectfully disagrees with the court in Levin that that is the prevailing case law across this country.

While there's much conviction of the judge in Levin to say they simply could have walked down the hallway and they talk about how many districts court judges would have been available, he also says in a footnote that many other jurisdictions -- and he doesn't seem to understand why -- they believe that the Rule 41 jurisdictional limitations apply to district court judges.

There is nothing that we've been able to

find in our research that indicates that somehow district court judges are free from the same limitations. And now I can't recall what the citation is, but I believe it's Federal Rule of Procedure 1, 2, or 3, which ultimately are going to say that the district court judges do not have this unbridled authority that Levin seems to argue they do.

THE COURT: But they certainly would have more authority than the magistrate judges because, as Gorsuch pointed out that in the concurrence that you mentioned in Krueger -- I mean, we've also got the Federal Magistrate Act to deal with here, which imposes jurisdictional and territorial limits on what a magistrate judge can do.

I mean, as a magistrate judge, I'm a magistrate judge of this district, but the district judges, I think, arguably are judges of the United States. They're appointed by the President and they sit in a particular district, but I don't know whether -- I'm not sure whether they would have the same sorts of limitations on them.

MR. HOFLAND: Yes, Your Honor. And I can say with certainty that the agents in the

Eastern District of Virginia, if somebody had came down with an opinion and there was case law supporting it, that you could simply get this from an unknown location if you go to a district court judge, they would have gone to a district court judge.

I don't think it's as clear as the judge indicates in Levin. From my last 18 months of being in this district practicing, I don't know a single instance in which a district court judge has issued a warrant.

THE COURT: I don't know that they've been asked to. But yeah, I agree that probably it hasn't happened.

MR. HOFLAND: So it's not clear to me that what the judge in Levin says applies. And he even drops a footnote where he indicates many other learned courts believe that the Rule 41(b) jurisdiction applies to district court judges as well as magistrate court judges.

So for what it's worth, if there is a -- if there's a small area of the law that says that district court judges can issue extraterritorial warrants, I imagine that there will be an uptick of warrants sought from district court judges for

situations like these. But even in that was available to the law enforcement in the Eastern District at the time, it's apparent that they weren't aware of that or else we would have attempted to cure that problem. So even that sort of question falls into a good-faith exception analysis.

So intentional and deliberate disregard for the rules, I think it's pretty clear that that hasn't been proven by the defense. The Rule 41 framework requires the defense to prove these harms, either prejudice or intentional and deliberate disregard. I don't believe, even from the briefing that touched on that, that we have intentional or deliberate disregard of any rule. The fact that we're talking about it the way we are indicates that -- that as a certainty it would be -- would be far beyond what it actually was.

THE COURT: I don't think there was much -- Mr. Widell, do you agree with that, that this is not an intentional and willful violation? Are you willing to concede that or --

MR. WIDELL: Your Honor, I think we'd prefer to stand on the -- on the brief.

THE COURT: Okay.

MR. HOFLAND: But then, Your Honor, there's a question of prejudice, and prejudice is taken up by all of these other districts that I mentioned that go through the Rule 41 --

THE COURT: Of the ones you mentioned, the four cases you mentioned, Michaud, Stamper, Levin, and then Epich, did any -- did they all find -- I know that in Michaud and Levin they did -- that the warrant was in violation of Rule 41?

MR. HOFLAND: They did, Your Honor. They all found that there was at least a technical violation of Rule 41. The Southern District of Ohio in Stamper effectively concurs almost across the board with the court in Michaud.

THE COURT: Okay.he did.

MR. HOFLAND: Epich is a little bit different in light of it being in the Seventh Circuit and the case law doesn't quite mirror up with ours. So to my recollection in Epich, because they rely upon good faith and they don't have the same analysis in the Rule 41 framework, I don't know that they reach prejudice.

THE COURT: They just find that what, that there was good faith -- that there was good faith for the -- again, I assume there was a second

warrant as there was here --

MR. HOFLAND: Yes, Your Honor.

THE COURT: -- based on the first one and that it was good faith to act upon that warrant? Or that --

MR. HOFLAND: They take up the NIT itself, Your Honor. So they say it's good faith that the NIT was achieved in the manner it was.

THE COURT: Okay.

MR. HOFLAND: To my knowledge, nobody has attempted to suppress on its own --

THE COURT: The second one.

MR. HOFLAND: -- the validity of the second warrant.

I put in my briefing there actually was a want to proceed with the NIT warrant, so when we're talking about second I understand you to mean the one in the local district.

THE COURT: Right. The Oklahoma warrant.

MR. HOFLAND: But when they take up the issue of prejudice, they take up the issue both times in favor of the United States in Michaud and in Stamper and they say that we don't have prejudice that would rise to suppression.

I understand the defense's argument to be because the warrant had this information, which is a violation, they couldn't have gotten the warrant, and if they couldn't have gotten the warrant, we wouldn't have the information to do a separate warrant.

The courts in both Michaud and Stamper, they both reject that as being the rein of prejudice because very clearly we're talking about a Rule 41 violation. And so if there is a problem with the warrant, basically every warrant would be invalidated and we wouldn't be able to get the information.

The defense invites us to say that we can't even go figure out how we could have cured it, it's simply that this one wasn't valid and this is the one that we used, so as a result it has to be everything invalidated. And the court says that that can't be the right reading of Rule 41 because we already are assuming a Rule 41 violation and then we're getting down to the issue of prejudice.

The interesting part is that both of these courts in Michaud and Stamper, they turn to the evidence being sought to determine prejudice. Because ultimately the information gleaned from the

NIT is not Mr. Arterbury's address or Mr. Arterbury himself, it is an IP address, an IP address which the user freely puts out on the Internet and must put out on the Internet in order to get any sort of Internet traffic. They freely share it with their Internet service provider who knows that information.

So when they come down on the issue of prejudice, effectively they're saying there is no prejudice because there's no reasonable expectation of privacy for the defendant in his IP address, he puts it out there even when he's going to this particular site. And to say that because it's encrypted now we add a level of privacy, can't be right because then we're simply saying if you conceal your criminal activity well enough, you're beyond the reach of the law.

THE COURT: Well, but if you're -- if you're conducting your criminal activity in your house, you would need a valid warrant to go into the house. I mean, sure, it's being concealed but you would need a valid warrant to get in there.

And isn't that the question here, whether this is a valid warrant to get into the computer and then get the information?

MR. HOFLAND: It's not when we're talking about an IP address. I mean, effectively an IP address is a house made of glass. The person in all of their activities are pushing out and emitting from their house what they're doing.

And so, too, did Mr. Arterbury in this case. When he navigated, even through the Tor network, he was pushing out to his Internet service provider and to the first entry node in these relay of nodes here's who I am. And there is a --

THE COURT: And then you sign up -- as I understand it, you sign up for the Tor network, as it were, and provide that basic information, and then from there on once you're part of that network or using that network, everybody understands that we're here to -- to cloak everything you do in anonymity so you can't -- you know, it will be very difficult to catch you.

MR. HOFLAND: That is true, Your Honor.

THE COURT: And as I read it, 80 percent of what's going on down there is child pornography related.

MR. HOFLAND: At least there's some articles and studies that suggest the same, yes, Your Honor.

THE COURT: All right.

MR. HOFLAND: The very fact of joining on this network, and understanding that there is an entry node who knows all of your information unencrypted and then at subsequent nodes that add layers of encryption all the way to the exit node, and then you can't see who that individual user is, the base activity that each authorizing user or each computer defendant is doing is going onto the Internet and thereby projecting who he or she is. And so as a result, routinely case law has been -- has been shown that there is no reasonable expectation of privacy in an IP address. So it's not a Fourth Amendment search when we obtain an IP address. Now, I understand that we have a little bit different case here, but at least as property being sought, there's no reasonable expectation of privacy in an IP address.

And so because of that, and we're taking up the issue of prejudice, these other courts have said that there is not prejudice when we're talking about, almost in a balancing manner, what the violation was with respect to what the information ultimately sought was. The NIT itself did not give us Mr. Arterbury. The NIT itself did not reach to

his address. It was, we received an IP address and further investigation needed to be done, an administrative subpoena had to be issued to an Internet service provider, and at that point we then have a specific user.

So just as the other courts have done and found no prejudice in light of the circumstances -- and I think we can get there by either talking about the lack of reasonable expectation of privacy in an IP address, something that he freely gives every time he goes on the Internet, or we can get there by talking about exigent circumstances -- was there another way for us to get this information? Sure. If the magistrate judge in the Eastern District of Virginia said, I'm not going to authorize that, I believe that this NIT still could have been sent out under exigent circumstances based upon the fleeting nature of the evidence and based upon the great harm that was occurring to young kids who were rescued from that harm, that as a result even if we -- that if this warrant hadn't existed, we still would have had exigent circumstances to send the NIT out over the network.

So for -- for those -- and what kind of goes hand in hand with that -- and I think I

already somewhat addressed it -- is this good faith and I think there's good faith all over this. I think if there's an ability to have a good-faith exception in this case, and we're not finding the way the Levin court did, but ab initio we don't there, then I think it's clear that Leon in good faith says these are people who are trying to use court authorization to do exactly what they did, not rely upon exigency, but use court authorization, the only place that they would have known how and where to go, and they sought a warrant.

So the good-faith exception applies. The fact that there is this new technology and one that criminal defendants are using to hide their criminal activity, that shouldn't inure to the benefit of those criminal defendants.

So for those reasons that I've laid out, I think barring any questions that you have now, I think that's it.

THE COURT: All right. Let me see if Mr. Widell has anything he wants to say in rebuttal.

MR. WIDELL: I think just briefly, Your Honor.

In regard to the exigent circumstances that's already been raised, that the government can't create the exigent circumstance, that amounts to a run-around the warrant for, and that's exactly what it did in this case.

The second thing is the IP address. To say that there is a bright-line rule that says an IP address is -- if I have my IP address written on a piece of paper and that piece of paper is in my house, and the government comes into my house and picks up that piece of paper without a warrant, they've done something that's suppressible regardless of whether I use my IP address publicly.

This is a case in which the individual didn't willingly give up his IP address. He did something exactly the opposite. He had an expectation of privacy at least in this instance. So --

THE COURT: But does it matter that what the defendant -- certainly in the government's view what the defendant is doing is hiding his activities arguably for illegal purposes?

MR. WIDELL: I don't -- I don't know why that would matter. Every criminal case that we've -- we get that's a Fourth Amendment case or a Fifth

Amendment case is a criminal purposes case. So I can't see why, you know, the Fourth Amendment applies to all of us.

I think that's all I want to say in rebuttal, Judge.

THE COURT: All right. Assuming that you're correct, that the pretrial has been moved, I'll check on that and see where we stand. But whatever I do on this, I'll try to do as quickly as I can, and then I'll need to probably shorten your time because I'm convinced that whichever way I go on this, there's going to be objections from somebody on the report and recommendation.

So would a week be sufficient? I mean, sounds like -- I mean, you've briefed this thing pretty authoritatively. I would I think you'd be basically presenting the same arguments to Judge Payne.

MR. WIDELL: Yes, sir. A week is fine.

THE COURT: Okay.

MR. HOFLAND: Yes, Your Honor. And I'm sorry. Just one other case cite for the sake of the premise that the IP address -- the use of Tor does not alter the public nature of the IP address.

In the Ninth Circuit -- again this is out

of Michaud's district -- United States v. Forrester, 512 F.3d -- I just have a citation at 510, that stands for an IP address belongs to the ISP, the Internet service provider, not the user.

And then Michaud itself --

THE COURT: Well, does that mean you would have to get the warrant to get -- well, it goes -- ultimately you do get the warrant for the ISP provider?

MR. HOFLAND: We do, Your Honor. Or at least an administrative subpoena.

THE COURT: But only because you've at least learned who the likely ISP -- when you get the information that comes from Arterbury's computer, you know the IP address. What does that enable you to do? Are you able to tell from that that it came from the Northern District of Oklahoma? Or what does that tell you exactly?

MR. HOFLAND: Yes, Your Honor. There are publicly available resources that allow you to put in an IP address and then push out what company, Internet service provider, owns that IP address and then also they can geolocate --

THE COURT: Geolocation. And so what happens then? The case -- somehow the case is

referred to authorities here in the Northern District for further action and they've got the IP address. They get the information they need. They're relying on probable cause established by the NIT warrant to come to Judge Wilson and say, based on what we -- what we gained through use of the NIT warrant, and now what we've gained through the administrative subpoena that was served on Cox Communications, we now know the physical address of the activating computer and we want a warrant to go in there and search that computer to see if there's child pornography.

MR. HOFLAND: That's right, Your Honor. And we agree that in terms of suppression, if the NIT warrant is suppressed, that was effectively wholly the basis of probable cause to get to that house.

THE COURT: Right.

MR. HOFLAND: But yes, Your Honor, the -- and maybe I didn't articulate it correctly, and certainly a review of the warrant, I think, lays this out -- but the Internet service provider owns the IP address and basically, you know, leases it to all of the users who connect through Cox or Comcast or otherwise, and then that is a unique

identifier for that person's actions but it's owned by the ISP.

And then Michaud, which we've talked about, but then also a case called United States v. Farrell from the Western District of Washington -- Farrell being F-a-r-r-e-l-l -- it's 2016 WL 705197. It, along with Michaud, takes up the idea that simply because a user uses Tor, it doesn't alter the premise that an IP address is owned by these ISP's and does not have a reasonable expectation of privacy in those IP addresses.

THE COURT: But you still have to get back to his computer to get the basic information that gets you to the ISP provider?

MR. HOFLAND: Yes, Your Honor. But when we're talking simply about the expectation of privacy and the information to be sought, there is none, even if he's using Tor.

MR. WIDELL: And from our perspective, the information was contained in the computer in the house.

THE COURT: Right.

MR. WIDELL: And so he had an expectation of privacy in what was in his house, particularly in what was in his computer. That's

it. Thanks.

THE COURT: I think that pretty well sums it up.

Okay. Thank you, gentlemen. It's an interesting issue. We'll try to get something out on this quickly so you can discuss it with Judge Payne.

MR. HOFLAND: Thank you, Your Honor.

THE COURT: Thanks.

(The proceedings were concluded)

C E R T I F I C A T E

I, Brian P. Neil, a Certified Court Reporter for the Northern District of Oklahoma, do hereby certify that the foregoing is a true and accurate transcription of my stenographic notes and is a true record of the proceedings held in above-captioned case.

I further certify that I am not employed by or related to any party to this action by blood or marriage and that I am in no way interested in the outcome of this matter.

In witness whereof, I have hereunto set my hand this 12th day of May 2016.

s/ Brian P. Neil

Brian P. Neil, RMR-CRR
United States Court Reporter